Chinese antivirus applications secretly collect user data

Google has removed from Play Store - then restored to its original state - one of the many anti-virus applications on mobile users, after Check Point security company discovered this application secretly collected user data collection.

Google has removed from Play Store - then restored to its original state - one of the many anti-virus applications on mobile users, after Check Point security company discovered this application secretly collected user data collection.

The application, called DU Antivirus Security, is a product of DU Group, a Baidu group company. According to the app's Play Store page, there are between 10 and 50 million people downloading and installing this application.

The application collects user data and switches to another application

In the report, researchers at Check Point said they found suspicious behavior in the way the application works. When the user first runs DU Antivirus Security, it will collect information such as:

1. Identity
2. Phonebook
3. Call history
4. Location information, if possible

DU Antivirus will then encrypt the data and send it to the remote server at 47.88.174.218. Initially, the researchers assumed that the server was under the control of the malware author but investigating DNS records and related subdomains showed that the host domain was registered under the name of an employee of Baidu is Zhan Liang Liu.

The following information will be used by another application belonging to the DU Group called Caller ID & Call BLock - DU Caller, with the aim of providing users with information about incoming calls.

Google removed and restored the clean version of the application

Check Point warned Google about this on August 21, removing the application on August 24. The application was later released on August 28 after DU Group deleted the code regarding the data collection.

Google deleted the application because it did not specify the data collection mechanism in the privacy policy nor did it ask the user for permission.

Check Point said that DU Antivirus Security v3.1.5 contains this code and it is possible that previous versions were available, but the company could not test the previous versions to confirm. Users should quickly update to the latest version.

Data collection mechanism found over 30 other applications

From the initial discovery, Check Point sought the appearance of this type of malicious code on other applications and found in 30 applications, 12 of which were on the official Google Play Store. Based on Google statistics, between 24 and 89 million users may have installed a data collection application without knowing it.

'These applications may execute code as an external library, transferring stolen data to DU Caller's remote server'. This is not the first time DU Caller has such behavior. Earlier this year, the application was discovered using various privacy policies to trick users and collect data whether they agreed or not.

Below is the name of the applications that contain the data collection code that Check Point discovered is located on the Play Store.

Package name	App name	Minimum downloads	Maximum downloads
com.duapps.antivirus	DU Antivirus Security - Applock & Privacy Guard	10,000,000	50,000,000
speedbooster.memoryoptimizer.phonecleaner.phonecooler	Memory Optimizer	5,000,000	10,000,000
com.coolermaster.cpucooler.coldown.free	Battery Cooler - Cooler Master	5,000,000	10,000,000
batterysaver.cleaner.speedbooster.taskmanager.phonecooler	Power Manager – Task Manager	1,000,000	5,000,000
com.antivirusguard.android	Antivirus Guard	1,000,000	5,000,000
ramoptimizer.phonecleaner.memorycleaner.speedbooster	RAM Optimizer	1,000,000	5,000,000
com.speedbooster.optimizer	RAM Master - Memory Optimizer	500,000	1,000,000
com.ramanalysis.booster	RAM Analysis	500,000	1,000,000
com.energymaster.batterysaver	Energy Master	500,000	1,000,000
com.internetanalysis.tool	Internet Analysis	100,000	500,000
com.coolertech.fastcooler	Fast Cooler – Phone Cooler	100,000	500,000
com.flashlight.led.hd.light.torch.bright	HD Flashlight - Bright & Free	100,000	500,000
com.cpucooler.coolermaster.coldown	CPU Cooler Master-Phone Cooler	50,000	100,000
Total		**24,850,000**	**89,600,000**

List of apps on Play Store that collect user data

Below is a list of applications that use the same code but outside the Play Store.

com.power.core.setting
com.friendivity.biohazard.mobo
com.energyprotector.tool
com.power.core.message
batterysaver.cleaner.speedbooster.taskkiller.phonecooler
com.rammanager.pro

com.memoryanalysis.speedbooster
com.whosthat.callerid
speedbooster.memorycleaner.phonecleaner.phonecooler
com.example.demos
com.android.fb
antivirus.mobilesecurity.antivirusfree.antivirusandroid
speedtest.networksecurity.internetbooster
com.ramreleaser.speedbooster
com.dianxinos.optimizer.duplay
com.coolkeeper.instacooler
com.memoryreleaser.booster
com.freepopularhotvideo.hotube